**Towards a dynamic file integrity monitor through a security classification**


ABSTRACT

File is a component of a computer system that has importance value of its own, either in terms of availability, integrity, confidentiality and functionality to a system and application. If unintended changes happen on the related file, it may affect the security of related computer system. File integrity monitor (FIM) tools is widely used to minimize the file security risk. This paper proposed dynamic schedule for FIM. This paper presents a dynamic scheduling for FIM by combining on-line and off-line monitoring based on related files security requirement. Files are divided based on their security level group and integrity monitoring schedule is defined based on related groups. The initial testing result shows that our system is effective in on-line detection of file modification.



**Keyword:** File integrity; HIDS; File security classification; Dynamic scheduling; Operating system